Technical Cybersecurity

GDB

GDB

GNU DEBUGGER

- ‣ Common
- ‣ Free
- ‣ Powerful!
- ‣ Tool of choice for application binary analysis
- ‣ The standard on Linux
  - ‣ …and by which other debuggers are judged

v. Static Analysis

STATIC ANALYSIS SHOWS YOU WHAT'S THERE

‣ Disassembly

‣ Decompilation

DYNAMIC ANALYSIS SHOWS YOU HOW IT WORKS

‣ PLT is empty prior to loading

‣ Sections moved around

‣ Calling sequence clear

Introducing GDB!